Secret nucléaire, information et participation citoyenne:

Martine Barré-Pépin, Marguerite Boutelet

Pre-print

Secret nucléaire, information et participation citoyenne

Secret nucléaire et secret-défense : considérations conclusives

Martine BARRÉ-PÉPIN et Marguerite BOUTELET

Le développement de l'industrie nucléaire en France est né de la volonté de certains, comme Pierre Guillaumat, de faire de la science de l'énergie atomique un instrument propre à conserver à la France son rang de grande puissance, puissance militaire et aussi industrielle. Quand, sur ce postulat, le CEA est créé en 1945, les recherches sur les applications de l'atome ont une finalité militaire et les applications civiles n'ont jamais été séparées des enjeux de défense car la technologie qui permet maîtriser l'atome à des fins militaires est la même que celle qui permet son utilisation civile. Si bien que, en matière nucléaire, le secret industriel est protégé par le secret défense. Depuis cette époque, le secret de la défense nationale a beaucoup évolué. Il a fait l'objet d'un encadrement plus précis et sa portée a été limitée par l'émergence du droit à l'information du public. Cependant, le lobby nucléaire a œuvré avec succès pour soustraire les activités nucléaires aux obligations de transparence introduites dans le droit commun des installations dangereuses pour l'environnement comme dans le droit des installations militaires non nucléaires. Aujourd'hui, ce secret même nucléaire est devenu un tigre de papier : malgré ses procédures, ses rituels, ses joutes avec les juges d'instruction ou avec les militants de Greenpeace, il est désuet devant la menace que constituent les attaques informatiques de toutes origines, y compris des services d'espionnage des grandes puissances alliées ou non. Si le secret défense, ainsi subverti par les nouvelles technologies, est impuissant à protéger le potentiel scientifique et technologique de la nation et les intérêts stratégiques de la France, pourquoi « le monde à part » du CEAEA y reste–il tellement attaché ? En dépit de sa lourdeur et de son coût, il conserve des avantages étrangers à la dissuasion nucléaire. Mettre à jour ces avantages non déclarés permet de vérifier que leur légitimité est aussi grande que celle qui s'attache à la transparence et d'envisager un nouveau compromis avec le droit à l'information du public.

I - Comment nucléaire rime-t-il avec secret[1] ?

Au CEAEA[2], le secret défense et le secret industriel et des affaires se confortent et parfois se confondent, constituant ensemble un secret particulier, le secret nucléaire. Le secret industriel couvre des intérêts aussi stratégiques que le secret militaire et pourtant il ne confère pas les

1 Cet intitulé en forme de question est inspiré des termes dans lesquels Jean-Marc Ayrault, alors président du groupe socialiste à l'Assemblée Nationale, a, en juin 2010, demandé officiellement au premier ministre François Fillon et au ministre de l'Industrie et l'énergie Eric Besson de rendre public le rapport de François Roussely sur « l'avenir du nucléaire français » classé secret-défense : « Il n'est pas sain que nucléaire rime avec secret et qu'il faille attendre les fuites dans la presse pour connaître le sens des préconisations qui ont été faites sur l'avenir de la filière industrielle française ».

2 Le Commissariat à l'énergie atomique et aux énergies alternatives est un établissement à caractère scientifique, technique et industriel, doté de la personnalité morale ainsi que de l'autonomie administrative et financière, Code de la recherche, Article L332-1 modifié par la loi N° 2010-237 du 9 mars 2010.

mêmes prérogatives. Alors que le secret de la défense se caractérise par l'indétermination de sa teneur, le formalisme des procédures de classification et d'habilitation et par son absolutisme – il est opposable sans justification -, le secret industriel, lui, doit être revendiqué par son détenteur à qui il appartient d'en établir la légitimité en montrant les conséquences dommageables d'une divulgation et sa portée est limitée par les tribunaux. Or, bien qu'obéissant à des régimes différents, le secret de la défense et le secret industriel, commercial et des affaires ont souvent un objet et des finalités identiques. Spécialement dans la filière nucléaire, de la recherche jusqu'aux applications tant civiles (énergie, santé, TIC) que militaires (armements), la dualité technologique fait que le secret industriel et commercial touche à la sécurité et à la défense de la nation française. Potentiellement sensibles et stratégiques, toutes les données et informations du secteur nucléaire mettent en jeu des intérêts fondamentaux[3]. Plus généralement, pour la défense et la sécurité économiques[4], les secrets d'entreprise sont d'intérêt public. Il s'agit à la fois de contrôler des biens et technologies à double usage et de préserver les infrastructures et les entreprises nationales contre l'espionnage, le sabotage et la concurrence. D'intérêt stratégique et économique national, les cibles privées et publiques, civiles ou militaires à défendre mobilisent les services de sécurité extérieure au Ministère de la Défense et les services de renseignement au Ministère de l'Intérieur[5]. Les secrets industriels, nucléaires ou non, sont également stratégiques. Ils doivent eux aussi être protégés comme les secrets militaires.

Les ingénieurs, fondateurs du CEA en 1945, ex-militaires pionniers du nucléaire, ont eu naturellement recours au secret de la défense pour protéger les recherches et applications civiles ou militaires sur lesquelles reposait l'avenir de la France. Ils ont tenu à en conserver l'usage si crucial face à la faible protection du secret industriel : afin que la protection des recherches et des savoir-faire qui constituent l'objet des secrets de l'industrie nucléaire soit autant que possible assurée par le secret défense. Ceci tient non seulement à l'histoire et au statut du Commissariat, omniprésent et omnipotent dans les institutions françaises, mais aussi à l'étendue de ses missions et domaines d'intervention. Acteur de la dissuasion nucléaire et de la sécurité nationale, le CEAEA mène des recherches dans le domaine de la Défense et de la sécurité[6]. Objectivement, le secret nucléaire est un secret industriel, au sens de technologie d'entreprise - savoir-faire, produits

3 Article 410-1 du code pénal : Les intérêts fondamentaux de la nation s'entendent (…) de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel.

4 De la défense économique à la sécurité économique active, Rapport Carayon, 2003.

5 Née en 2008 de la fusion des renseignements généraux (RG) et de la DST (contre-espionnage), la DCRI, Direction centrale du renseignement intérieur, est comprise comme le pendant de la Direction générale de la sécurité extérieure (DGSE) du ministère de la Défense. Selon les propos du Ministre Manuel Valls qui, en janvier 2013, en annonçait la transformation en une Direction Générale de la sécurité intérieure (DGSI) placée directement sous son autorité, «ses missions s(er)ont exclusivement fondées sur la défense de la souveraineté nationale, des intérêts fondamentaux de la Nation et de l'intégrité des institutions républicaines». Réforme du renseignement intérieur : M. Valls choisit la continuité, Le Monde 18 juin 2013.

6 Avec « pour mission de concevoir, fabriquer, maintenir en condition opérationnelle puis démanteler les têtes nucléaires qui équipent les forces océaniques et aéroportées françaises. A cette fin, une des priorités du CEA est de mettre en œuvre le programme Simulation. Il est chargé de la conception et de la réalisation des réacteurs nucléaires équipant les bâtiments de la Marine nationale, sous-marins et porte-avions. Il apporte son soutien à la Marine nationale pour le suivi en service et le maintien en conditions opérationnelles de ces réacteurs. Il est également responsable de l'approvisionnement des matières nucléaires pour les besoins de la Défense. Le suivi de l'impact sur l'environnement de ses activités fait l'objet d'une attention soutenue. Dans un monde en profonde mutation, le CEA contribue à la sécurité à travers l'appui technique qu'il apporte aux autorités, pour les questions de désarmement, de lutte contre la prolifération nucléaire et le terrorisme. Depuis l'intégration du centre de Gramat au CEA en 2010, la défense conventionnelle fait partie de ses nouvelles activités. Pour mener à bien ses missions, le CEA est responsable des études scientifiques et techniques de base, ciblées sur les programmes Défense ».

et procédés propres à la filière – spécialement dans ce secteur à caractère éminemment stratégique. Au sein du CEAEA, la filière nucléaire intègre la recherche scientifique en amont et le développement technologique en aval avec des centaines d'entreprises ou start-up et de multiples applications – la distinction civil/militaire n'ayant, à ces différents niveaux, aucun fondement ni pertinence. Il s'agit plus largement d'un secret commercial et des affaires relatif aux programmes en cours et aux projets, organisé dans les relations internes et externes du CEAEA, maintenu en interne dans chacun des dix centres CEA et à l'extérieur avec l'État[7] et les collectivités locales, des fournisseurs, développeurs et prestataires sous-traitants, leurs 53 partenaires académiques, des organismes de recherche, et plus de 500 partenaires industriels[8]. Formellement, les données technologiques sensibles et les informations stratégiques peuvent revêtir le sceau du secret de la défense. Pour ce qu'il recèle de potentialités susceptibles de mettre en jeu les intérêts fondamentaux de puissance nucléaire et d'autonomie énergétique de la France, le secret industriel et des affaires est sinon toujours compris, du moins compréhensible dans le régime formaliste de classification et d'habilitation secret-défense. Si, en 1945, pour protéger les recherches sur les applications civiles et militaires de l'atome, le recours au secret défense était justifié, cette solution est moins fondée aujourd'hui.

Il existe en effet d'autres procédés que le secret défense pour protéger les intérêts stratégiques de la France en matière de recherche et de développement de technologies nouvelles. Le maintien au secret des demandes de brevet d'invention d'une part, le dispositif de protection du potentiel scientifique et technique d'autre part, sont les principaux moyens du droit commun. Une invention étant potentiellement stratégique, l'autorité militaire peut en contrôler l'usage et la divulgation en bloquant la demande de brevet. Dans la guerre économique mondiale comme dans les rapports de souveraineté interétatiques, ce sont bien les potentialités de développement technologique en matière nucléaire et les possibilités d'applications industrielles de l'atome qui sont en jeu. Pour les technologies duales en particulier, la position du curseur distinctif des applications industrielles civiles et de défense et le moment du passage ou de l'extension de l'une à l'autre sont également d'intérêt stratégique. Le régime légal de la propriété intellectuelle et la procédure de brevetabilité des inventions en offrent la démonstration puisque toute invention de produit ou de procédé qui fait l'objet d'une demande de brevet à l'INPI est mise au secret pour examen par le Ministre chargé de la défense. Ce dernier peut en empêcher la délivrance et la divulgation. D'ordre public, ce dispositif confère à l'Etat le pouvoir de contrôler la destination, autrement dit les usages, qu'ils soient civils ou militaires, des inventions, voire de les réquisitionner et d'empêcher l'octroi d'un titre de propriété à effet territorial mais avec publicité mondiale de la description de l'invention et des revendications. L'habilitation du ministre de la défense à prendre connaissance de techniques innovantes avant qu'elles ne soient divulguées et exploitées est une prérogative de souveraineté[9]. Ce contrôle ne porte cependant que sur des

7 Comme le CNES, Agence spatiale civile, le CEAEA est sous la tutelle du Ministère de l'enseignement supérieur et de la recherche.

8 http://www.cea.fr/

9 Code de la propriété intellectuelle, Article L612-8 : Le ministre chargé de la défense est habilité à prendre connaissance auprès de l'INPI, à titre confidentiel, des demandes de brevet.

Paradoxalement, c'est lorsque le possesseur d'une technologie jusqu'alors tenue secrète en revendique la priorité et le monopole d'exploitation pour une application industrielle que les autorités militaires interviennent et interrompent provisoirement – parfois définitivement - le cours de la demande de brevet à l'INPI, ce qui empêche la publication de la description (Articles L612-9 et L612-10 du code de la propriété intellectuelle).

L'entretien avec la responsable du Département de PI d'un grand groupe industriel montre, d'un côté, les conditions de tri préventif ou conservatoire par le Ministre de la défense et de classification « au large » des inventions par des experts habilités secret-défense dans les locaux de l'INPI et, de l'autre côté, préalables au dépôt de demandes de brevet, les stratégies d'évitement de la part des industriels des secteurs de technologies à double usage, tels que le nucléaire civil ou non. « Pour les opérateurs, il y a une stratégie d'esquive, alors que de la part de la DGA, il s'agit de surveiller des données sensibles qui évoluent avec la technique ».

technologies assez développées - susceptibles d'application industrielle - dont les détenteurs sont candidats au monopole temporaire d'exploitation et prêts à renoncer à les garder secrètes.

En revanche, la protection du potentiel scientifique et technique de la nation est assurée par un dispositif général, à caractère préventif et dissuasif, assez proche tant sur le plan technique que pénal de celui du secret défense, sans toutefois le cérémonial ni l'arbitraire du régime dérogatoire en question. La notion de patrimoine, désormais étendue à celle de potentiel scientifique et technique de la nation transcende la distinction des deux secrets, secret industriel et secret de la défense[10] comme le montrent les quatre risques identifiés au titre de la protection du potentiel scientifique et technique (PPST)[11]. Des dispositions générales et aussi spéciales[12] punissent et préviennent la communication à l'étranger de documents ou de renseignements d'ordre économique, commercial, industriel, financier ou technique non classifiés secret défense, cependant de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public. La protection pénale contre les atteintes aux intérêts fondamentaux de la nation[13] pour les délits de trahison, espionnage, intelligences avec une puissance étrangère, notamment par livraison d'informations[14], est assortie d'une protection administrative et physique. Des « zones à régime restrictif » (ZRR)[15] sont délimitées[16] et le

10 Le potentiel scientifique et technique de la nation est notamment constitué de l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée et au développement technologique. Ce potentiel constitue l'un des éléments des intérêts fondamentaux de la nation mentionnés par l'article 410-1 du code pénal.

11 Circulaire interministérielle du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la Nation. N° 3415/SGDSN/AISTfPST.

L'article R.413-5-1 du code pénal vise à prévenir le détournement des savoirs et savoir-faire en organisant la protection du potentiel scientifique et technique de la nation au regard des quatre risques suivants :

risque 1 (RI), «intérêts économiques de la Nation» : concerne les atteintes au potentiel scientifique et technique susceptibles de nuire aux intérêts économiques de la Nation ;

risque 2 (R2), «arsenal militaire» : concerne le détournement du potentiel scientifique et technique susceptible de renforcer l'arsenal militaire (conventionnel) d'un autre pays ou d'affaiblir les capacités de défense de la nation ;

risque 3 (R3), «prolifération» : concerne la prolifération des armes de destruction massive et de leurs vecteurs, dans les domaines nucléaire, balistique, chimique ou biologique ;

risque 4 (R4), «terrorisme» : concerne le détournement de savoirs susceptibles d'être utilisés à des fins d'activités terroristes, menées sur le territoire national ou à l'étranger (ce risque comprend également le risque radiologique).

12 Telle la Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, dite « loi de blocage ».

13 Code pénal, Article 410-1, définition des intérêts fondamentaux de la Nation.

14 Visés aux articles 411-1 et suivants du code pénal. Introduits dans le code pénal en 1995, les article 411-6 et suivants répriment les faits d'espionnage dont les auteurs encourent des peines de quinze ans de détention criminelle et 225 000 euros d'amende lorsqu'ils portent atteinte à l'intérêt d'entreprises nationales clés par « livraison à une entreprise étrangère de renseignements dont l'exploitation et la divulgation sont de nature à porter atteinte aux intérêts fondamentaux de la Nation ».

15 Le dispositif de protection du patrimoine scientifique et technique qui procédait d'une démarche relativement ancienne, une vingtaine d'années, était fondé sur une base juridique faible, une simple instruction ministérielle. Limité aux étrangers hors Union européenne, il était difficile à mettre en œuvre. À la suite d'un audit de 2009 soulignant que le support du savoir est passé du papier au virtuel, il a été actualisé par Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413- 7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation. Assuré par la mise en place, dans les secteurs scientifiques et techniques protégés en raison des intérêts pour la nation, de zones à régime restrictif (ZRR) et dans les laboratoires des spécialités les plus sensibles du secteur public et du secteur privé, il s'applique à tous les chercheurs, quelle que soit leur nationalité, Ph. Gasnot, Fonctionnaire de Sécurité et Défense du CNRS, Présentation de la PPST, Comité technique, 20 juin 2013, www.sud-**recherche**.org/.../IMG/.../pointC1_presentation_PPST.pdf). La liste des secteurs protégés et spécialités sensibles (ZRR) figure à l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation. Cf. *Livre blanc Défense et sécurité nationale* 2013, p. 107.

16 Dans l'affaire Michelin, le délit d'espionnage n'a pas été retenu en l'absence de preuve que les informations proposées « présentaient un caractère à ce point stratégique », étant jugé que « le seul fait du classement du centre de

contrôle de l'accès à ces lieux est organisé par concertation entre les pouvoirs publics et les chefs des services, établissements ou entreprises concernés[17]. Le dispositif de protection du potentiel scientifique et technique s'intègre dans l'ensemble des régimes participant à la sécurité de la nation. Protection du secret de la défense nationale et protection du potentiel scientifique et technique, les deux dispositifs ont censément des champs d'action complémentaires : protection d'une information classifiée de défense et protection de savoirs et savoir-faire sensibles qui ne relèvent pas nécessairement de ce domaine. Leurs procédures sont compatibles : elles établissent pour les personnes habilitées une exemption de l'avis ministériel nécessaire pour entrer dans une ZRR. Ainsi, les locaux du Laboratoire Interdisciplinaire Carnot de Bourgogne[18] qui effectue des recherches en collaboration avec le CEA du Valduc sont une zone à régime restrictif d'accès. Le Haut fonctionnaire de défense et sécurité (H.F.D.S.) y intervient régulièrement non pas à raison de sa collaboration avec le centre de Valduc mais à cause des risques d'atteinte au potentiel scientifique et technique dans les échanges internationaux. Le secret défense ne s'y impose qu'exceptionnellement pour certains travaux dont le directeur et les chercheurs n'ont pas à connaître[19]. En revanche, tous les contrats industriels relèvent de l'Intelligence économique[20]. Et le laboratoire fait l'objet d'un contrôle permanent de la Direction Centrale du Renseignement Intérieur (DCRI). En outre, la sécurité informatique y est essentielle et le Système de Sécurité de l'Information (SSI) très contraignant. Aujourd'hui, grâce au système de PPST, il est heureux que les laboratoires de recherche puissent se protéger contre les actes d'espionnage sans avoir recours au secret défense.

Comme le secret défense, néanmoins, ces protections sont elles aussi limitées ou subverties par les possibilités d'interception et de diffusion qu'offrent les technologies de l'information et de la communication. En premier lieu, l'innovation immatérielle, programmes et fichiers de résultats, échappe au système territorial de brevet. En effet, légalement, s'agissant d'information non brevetable, le contrôle par le ministre de la défense de la destination lié à la procédure de délivrance et conditionnant l'octroi du titre de propriété est inapplicable aux créations logicielles et aux bases de données. Techniquement, l'hégémonie du réseau transnational des télécommunications permet des atteintes aux secrets privés et aux prérogatives de souveraineté des États. D'un côté, l'affaire WeakyLeaks et celle du soldat américain analyste du renseignement

---

recherches en établissement à régime restrictif n'induit pas nécessairement que des éléments du potentiel économique de la France, au titre de l'article 410-1 du code pénal, soient concernés ». Les faits ont été déqualifiés en « collecte irrégulière de documents ».

17 L'article 413-7 du code pénal qui réprime le fait de s'introduire, sans autorisation, à l'intérieur des locaux et terrains intéressant la défense nationale et qui sont clos en vue d'assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications vise également à la préservation du potentiel scientifique et technique de la. Nation. Cet article prévoit qu'un décret en Conseil d'Etat détermine les conditions dans lesquelles il est procédé à la délimitation des locaux et terrains visés ainsi que les conditions dans lesquelles les autorisations d'y pénétrer peuvent être délivrées. C'est l'objet du décret N° 2011-1425 du 2 novembre 2011 et des deux arrêtés du 3 juillet 2012, dont l'un n'est pas publié au J.O.

18 ICB (UMR 5205), Entretien du 5 mai 2011 sur le secret défense et le secret industriel dans les coopérations de recherche avec le CEA du Valus, avec le Directeur, Gilles Bertrand, Professeur de chimie-physique, Président de l'Université de Bourgogne (1988-1993).

19 Seuls trois ou quatre membres de l'ICB sont habilités secret-défense parmi lesquels le conseiller scientifique de la culture au Valduc.

20 L'intelligence économique s'est développée et organisée en trois temps avec le rapport Martre, Intelligence économique et stratégie des entreprises en 1994, le rapport Carayon, Intelligence économique, compétitivité et cohésion sociale en 2003, et l'institution d'un Délégué interministériel à l'Intelligence économique, Olivier Buquen nommé en septembre 2009. À la suite du rapport Carayon, le gouvernement avait nommé un Haut Responsable chargé de l'Intelligence économique (HRIE), rattaché au Secrétariat général de la défense nationale et chargé d'impulser et de coordonner une politique publique d'intelligence économique. Alain Juillet a exercé la fonction jusqu'en mai 2009. Désormais directement rattachée au Premier ministre, Madame Claude Revel a été nommée déléguée interministérielle à l'intelligence économique le 29 mai 2013.

militaire, Bradley Manning, son principal informateur qui a fourni quelques 700.000 documents militaires et diplomatiques, sont emblématiques de la vulnérabilité des systèmes de sécurité et des menaces pesant sur les secrets d'État. De l'autre, provoqué par les révélations d'un ancien employé de la CIA, Edward Snowden, sur le programme du renseignement américain PRISM, le « scandale des écoutes électroniques multinationales » met à jour les actes d'espionnage et la surveillance d'Internet par les agences de renseignement américaine, la NSA, et aussi française[21] et britannique[22]. Il montre d'une part l'existence du système anglo-saxon d'accès à la quasi-totalité des communications civiles et militaires par siphonage et duplication des données du Net et d'autre part la légalité en droit américain de la cybersurveillance secrète des réseaux téléphoniques dans et hors des Etats-Unis[23]. Les actes d'espionnage ainsi dénoncés sont commis par des agences de renseignement à caractère étatique, au nom de la souveraineté et avec des moyens techniques et logistiques hors du commun[24]. Constamment sous la menace d'une attaque informatique multiforme[25], les infrastructures vitales comme les activités économiques et sociales sont exposées à des risques majeurs[26] dont le secret défense ne les protège pas.

Inapplicable aux objets, documents et emplacements situés hors de nos frontières, le secret défense est en pratique inefficient vis-à-vis des puissances étrangères. Il n'est qu'à constater sa lourdeur et son inadaptation à la réalité des marchés[27], tous échanges commerciaux et flux électroniques confondus. Il convient surtout de le comparer au système de contrôle des exportations de matériel militaire par les Etats-Unis. Les règles ITAR[28] qu'il est d'ailleurs question de moderniser ou de réformer à raison de leur caractère par trop contraignant[29] ont un champ d'application qui comprend logiquement les technologies duales mais aussi les projets de recherche, les plans et les composants qui y sont attachés. Et le concept "d'exportation" est largement étendu, à l'extérieur des Etats-Unis et également, à l'intérieur du territoire américain, aux étrangers qui travaillent pour des compagnies américaines. Grâce à ce système qui interdit aux opérateurs de réexporter sans autorisation les composants américains, parce qu'ils sont compris dans les objets et services liés à la défense nationale, et donc d'en acheter à des

21 Jacques Follorou et Franck Johannès, R2vélations sur le Big Brother français, La DGSE collecte et stocke l'ensemble des communications électromagnétiques, en dehors de tout contrôle ; Questions à …. Arnaud Danjean, président (UMP) de la sous-commission sécurité et défense au Parlement européen, « Tous les services de renseignement occidentaux s'espionnent », Le Monde 5 juillet 2013.

22 Sur l'espionnage international et le système mondial d'écoutes électroniques multinationales créé après la guerre après des traités secrets entre les Etats-Unis et le Royaume-Uni, lire Duncan Campbell, Le Royaume-Uni, maître-espion, Le Monde 2 juillet 2013. Et aussi, Nathalie Guibert, Derrière l'antiterrorisme, l'espionnage industriel, Le Monde 2 juillet 2013.

23 La loi FISAA (Foreign Intelligence Surveillance Amendements Act) de 2008 sur le renseignement extérieur autorise le gouvernement américain à émettre des injonctions judiciaires secrètes aux compagnies informatiques américaines alors tenues de lui remettre toutes leurs données provenant de l'étranger.

24 Enquête, Les « grandes oreilles » de l'Amérique, Etats-Unis, Ph. Bernard, Voyage au cœur de la NSA, À l'automne doit être inauguré le centre d'interception des communications de Bluffdale (Utah). Un « big data center » aux capacités titanesques, construit dans le secret, Le Monde géo&politique, 29 août 2013.

25 Blocages malveillants, destruction matérielle, neutralisation d'un système, vol ou altération de données, prise de contrôle à des fins hostiles ; cf. Instruction ministérielle interministérielle n°1300 sur la protection du secret de la défense nationale, 30 novembre 2011, p.6.

26 « La croissance continue de la menace, l'importance sans cesse accrue des systèmes d'information dans la vie de nos sociétés et l'évolution très rapide des technologies …. imposent aujourd'hui d'augmenter… le niveau de sécurité et les moyens de défense de nos systèmes d'information, tant pour le maintien de notre souveraineté que pour la défense de notre économie et de l'emploi en France », *Livre blanc Défense et sécurité nationale,* 2013, p. 105.

27 L'instruction générale interministérielle N°1300 sur la protection du secret de la défense nationale n'évoque pas une seule fois, dans les articles consacrés aux annexes de sécurité dans les contrats, la question de l'exportation de matériels comportant des technologies sensibles.

28 International Traffic in Arms Regulations,

29 Sur l'actualité, on peut consulter le blog d'O.-P. Jacquotte consacré au système américain de contrôle des exportations et à sa réforme, ITAR EAR, USML, CCL, La réforme en cours, http://globalreachsas.blogspot.fr/

fournisseurs qui n'en demandent pas licence, les Etats-Unis contrôlent effectivement l'usage de leur technologie dans le monde.

La vulnérabilité des systèmes ou réseaux affecte indifféremment les secrets privés et les secrets d'État. La sécurité de l'information exige une protection physique de données et fichiers, des verrouillages et codes d'accès et des procédés de chiffrement qui relevaient du régime des armes jusqu'à la libéralisation des services cryptologie. Et les atteintes aux systèmes informatiques[30], intrusions par accès et maintien frauduleux, piratages, altérations et divulgations sont aussi le fait de « hackers »[31] et de simples usagers. Dans ce contexte, une situation paradoxale s'est instaurée où, d'un côté, des secrets d'État sont contestés et doivent justifier leur légitimité, de l'autre, des secrets privés que la puissance publique est incitée à protéger s'affirment tandis que se multiplient des stratégies de « dissémination volontaire »[32] susceptibles de contrarier les objectifs de sécurité de l'État[33]. Les raisons d'Etat s'évanouissent-elles devant celles de réseaux infra ou supranationaux[34] ? Et, derrière la lutte contre le terrorisme, n'est-ce pas l'espionnage industriel qui se profile[35] ? Si la protection des secrets des entreprises privées n'est pas suffisante, elle ne le serait pas davantage par le secret défense.

Réclamées par les milieux d'affaires**,** une « meilleure » protection et la pénalisation de la violation du secret des affaires ont fait l'actualité législative il y a quelques mois. Une protection formelle analogue à celle du secret-défense, par un système d'estampillage, est d'ailleurs prévue. Pour l'heure, l'adoption le 23 janvier 2012 par l'Assemblée Nationale de la proposition du député Carayon visant à sanctionner la violation du secret des affaires reste une tentative de renforcer la protection des secrets d'entreprises. Néanmoins, sans l'analyser comme un véritable changement de nature des enjeux liés aux secrets – intérêts stratégiques de la nation et/ou intérêts privés des entreprises – en une relative confusion de leurs domaines et caractères respectifs[36], il faut surtout y voir la prétention des opérateurs privés à disposer d'un marquage arbitraire et symbolique qui leur servirait plus à signifier leur puissance et à dissuader par l'évocation des pénalités encourues qu'à prévenir des atteintes et à protéger utilement des documents et données confidentiels.

Compte tenu des enjeux de cyberdéfense et des pratiques de veille technologique[37], d'intelligence

30 Code pénal, Articles 323-1 à 323-6 modifiés et complétés par la loi du 21 juin 2004 pour la confiance dans l'économie numérique, Lutte contre la cybercriminalité.

31 Un hacker chinois s'est introduit dans le système informatique du Pentagone où il a pu consulter les prototypes d'armement, déchiffrer et copier les plans et les projections stratégiques sur vingt-cinq ans. « Des hackers chinois ont pénétré les systèmes informatiques du Pentagone », Le Monde.fr 28 mai 2013. Cyberdéfense : la France reconnaît son retard, Le Monde.fr 3 juin 2013.

En février 2012, un sous-traitant informatique soupçonné d'avoir commis un vol important de données confidentielles dans un centre du CEA a été placé en garde à vue au siège de la DCRI. Identifié à la suite d'une plainte des services de sécurité du CEA, le suspect avait fait l'objet d'une surveillance pour connaître ses éventuels contacts. Situé à Bruyères-le-Chatel (Essonne), ce centre est spécialisé dans le calcul de haut niveau. Ses ordinateurs sont utilisés dans des recherches sur la sûreté des réacteurs nucléaires, l'imagerie médicale et la climatologie.

32 Par des systèmes ouverts, logiciels libres et publications web de type WeakyLeaks.

33 Bertrand Warusfel, Colloque Image et usages du secret, Belfort 2003, Document de présentation transmis par l'auteur.

34 André Glucksmann, Le cyberespionnage nous projette dans une ère de confrontations sans limites, Le Monde 3 juillet 2013.

35 N. Guibert, Derrière l'antiterrorisme, l'espionnage industriel, Le Monde 2 juillet 2013.

36 Le vote en l'état de la proposition de loi visant à sanctionner la violation du secret des affaires est inconcevable en ce qu'elle prévoit la possibilité de classifier un document dès lors que sa divulgation serait « de nature à compromettre gravement les intérêts de l'entreprise » : assortie d'une condition aussi imprécise, la transposition d'un système totalement inadapté aux réalités de l'entreprise comporte un risque évident de sur-classement des informations confidentielles.

37 Sur les sociétés de « sécurité offensive », Enquête, Yves Eudes, Hackers d'État, Le Monde 20 février 2013.

économique[38] et du renseignement dans le contexte global, le constat de l'inefficacité du régime national et formaliste du secret défense semble s'imposer. Aussi anachronique, désuet et inadapté soit-il au regard des menaces que les technologies de l'information et de la toile font peser sur nos sociétés, sa fonction symbolique n'en paraît que plus grande. Essentielle même. Car le secret défense manifeste l'importance que l'État attache aux objets qu'il est censé protéger, aux applications civiles et militaires de l'atome. Et il fait participer à la grandeur de la France chaque personne gratifiée du poids de l'habilitation. Avec le label secret-défense, la visibilité des enjeux stratégiques du nucléaire prévaut sur la transparence des stratégies et la lisibilité des programmes de sécurité. Aussi, puisqu'il s'agit de stratégies, dissuasion et persuasion, le secret industriel et des affaires nucléaire se pare-t-il largement – et sans doute abusivement au regard des objectifs et règles de sécurité environnementale - des formes du secret-défense. Il s'exerce dans des conditions dérogatoires, comme un « donner à voir » sinon un gadget à usage intérieur, à effet limité au territoire français. Il s'y impose néanmoins comme motif absolu - sans besoin de justifier d'aucune légitimité - de refus de communiquer des documents administratifs.

Face aux nouvelles formes d'espionnage, le secret défense dont se sert le CEAEA pour couvrir des informations relevant du secret industriel n'assure pas une protection plus efficace que celle dont bénéficie le patrimoine scientifique et technique. Le vrai défi d'aujourd'hui, la mise en place des règles de sécurité des systèmes d'information adaptées à l'évolution des techniques et le développement d'une expertise diffusée après de tous les acteurs publics ou privés, est hors de portée du secret défense. Dans ce contexte, l'attachement du « lobby nucléaire » au maintien de la soumission des activités nucléaires au secret défense interroge.

II – Pourquoi invoquer aujourd'hui le secret défense aux fins de soustraire les activités nucléaires aux obligations de transparence ?

Le maintien des activités nucléaires sous le régime du secret défense n'est pas un oubli. Le choix fait en 1945 s'est maintenu au fil des réformes jusqu'à ces dernières années. Les contraintes, les coûts et l'inutilité d'un système dépassé n'y ont rien changé. Les quelques avantages, pas toujours avouables, que conserve le secret défense pour les activités nucléaires militaires suffisent-ils à conférer à ce secret une légitimité prévalant sur la légitimité du public à connaître les conséquences des activités nucléaires militaires sur sa santé et son environnement ? Les installations militaires et les sites nucléaires ont dû progressivement se plier à l'obligation d'information et de participation du public résultant des textes internationaux, de la Convention d'Aarhus notamment. Les installations classées intéressant la défense nationale sont soumises au droit commun des installations classées tel qu'il est prévu par le code de l'environnement moyennant quelques exceptions pour les installations réalisées dans le cadre d'opérations secrètes intéressant la défense nationale : il est seulement prévu à l'article R. 317-3 du code de l'environnement que le préfet disjoint du dossier soumis à l'enquête ou aux consultations les éléments de nature à entraîner la divulgation de secrets de défense nationale dans le domaine militaire ou industriel. Cependant, les installations nucléaires civiles et militaires sont exclues du

38 La frontière peut être parfois mince entre veille et espionnage. On sait que les veilleurs se cantonnent à l'exploitation de l'information blanche (publiée) et grise (diffusée) et ne doivent jamais aller sur le terrain de l'information noire (Sûreté de l'État, défense, sécurité publique, mais aussi secret de fabrique et les nombreux secrets professionnels variant d'un métier à l'autre, et les savoir-faire protégés). Dans ce contexte, passer la frontière de l'information noire entraîne le plus souvent des risques pénaux, doublés de risques civils puisque les victimes pourront demander à être indemnisées.
http://www.les-infostrateges.com/article/1012367/aspects-juridiques-des-fonctions-de-veille

champ d'application de la police des installations classées pour la protection de l'environnement. Les installations nucléaires de base sont soumises depuis 1963 à une réglementation spécifique distincte du droit commun des installations classées. La loi transparence et sécurité nucléaire de juin 2006 a maintenu ce particularisme tout en aménageant un droit à l'information du public[39] : le droit d'être informé sur les risques liés aux activités nucléaires, à leur impact sur la santé et la sécurité des personnes ainsi que sur l'environnement. Le texte mentionne en outre le droit d'être informé sur les rejets d'effluents des installations[40].

Cependant, comme le prévoyait déjà l'article 17 décret du 11 décembre 1963 relatif aux installations nucléaires, les dispositions de la loi transparence et sécurité nucléaire ne sont pas applicables aux installations nucléaires intéressant la défense.[41] Le code de la défense prévoit pour les installations nucléaires de base secrètes un régime dérogatoire qui réserve entièrement aux ministres de la défense et de l'industrie la décision d'autorisation d'une installation nucléaire de base secrète. L'instruction du dossier et le contrôle des installations est confié au DSDN (délégué à la sûreté nucléaire et à la radioprotection pour les activités et installations intéressant la défense) assisté de l'inspecteur des armements nucléaires. Dans la procédure d'autorisation de création d'une installation nouvelle, aucune enquête publique n'est prévue[42] alors que celle-ci permet de communiquer au public les informations sur les conséquences sur l'environnement des activités dangereuses en projet. Les commissions locales d'information y sont remplacées par des commissions d'information[43] dont la composition[44] et les missions sont soigneusement limitées. Ces commissions spéciales ne semblent avoir aucune capacité d'autonomie. Elles sont convoquées une fois par an par le préfet pour entendre le rapport de sûreté. Leur fonctionnement ne donne pas satisfaction aux associations qui en font partie[45]. Cette volonté de se soustraire aux règles de transparence prévues pour les autres installations industrielles ou nucléaires surprend parce que les règles prévues par ces textes spéciaux comportent à peu près les mêmes dispositions, sauf que tout examen non militaire des projets est exclu : les dossiers sont instruits par des autorités militaires et les installations contrôlées par des fonctionnaires du ministère de la

39 Loi n° 2006-686 du 13 juin 2006 relative à la transparence et à la sécurité nucléaire , article 2-II-2°.

40 L'information du public repose sur trois piliers, le rapport de sûreté, les commissions locales d'information et le haut comité à la transparence et à la sûreté nucléaire. Les exploitants doivent établir une fois par an un rapport de sûreté qui porte sur les dispositions prise en matière de sûreté, les incidents et accidents en matière de sûreté nucléaire, les résultats des mesures des rejets radioactifs et non radioactifs de l'installation, la nature et la quantité de déchets radioactifs entreposés sur le site de l'installation. Des commissions locales d'information sont instituées pour exercer une mission générale de suivi, d'information et de concertation en matière de sûreté nucléaire et assurer une large diffusion de ses travaux

41 Article 2 alinéa 3 de la loi relative à la transparence et à la sécurité nucléaire.

42 Sauf pour les demandes d'autorisation de rejets liquides ou gazeux et de prélèvements d'eau (DARPE) sous réserve, selon l'article R1333-51-1 du code de la défense, que les éléments de nature à entraîner la divulgation de secrets de la défense nationale soient retirés du dossier soumis à enquête. Encore faut-il observer que, même pour les autorisations de prélèvement d'eau, l'enquête publique est exclue lorsque qu'il s'agit d'opérations couvertes par le secret de la défense nationale.

43 Créés par le décret n° 2001-592 du 5 juillet 2001 relatif à la sûreté et à la radioprotection des installations et activités nucléaires intéressant la défense codifié aux articles R 1333- 37 et suivants du code de la défense.

44 Les associations de protection de l'environnement, les représentants de l'Etat et des collectivités locales des autorités militaires et des exploitants comme le CEA. Le préfet nomme tous les membres y compris associatifs sauf les représentants des collectivités locales. Article R. 1333-38 et R.1333-39 du code de la défense.

45 Les services de la préfecture de Dijon ont ainsi été condamnés par le tribunal administratif de Dijon à communiquer les comptes rendus des commissions d'information du centre de Valduc, cf. T.A. Dijon, 17 juin 2010, n° 0902408, Alain Caignol. D'autres commissions des installations secrètes rencontrent aussi des difficultés. À la commission d'information de Brest et l'Île longue, les associations se plaignent du refus d'organiser un exercice d'évacuation de la population de Brest, de la maigreur des dispositions du PPI ; à Toulon, de l'absence de contradicteur compétent au sein de la commission, de ce que personne n'est capable de comprendre les informations données ; à Cherbourg, de l'absence d'écoute des associations. Cf. Jean Marie Collin, « Nucléaire : et si on s'intéressait aux installations militaires secrètes », Bastamag, 12 février 2012, www.bastamag.net/article2084.html

défense. La dispense d'information du public étonne alors que cette information existe, qu'elle est nécessaire, surtout lorsqu'elle implique la participation des populations comme les exercices de secours en cas d'accident. La consultation des procès verbaux de commissions d'information révèle que la communication est assez soignée même si c'est une information unilatérale et que les analyses des effluents sont faites en interne et non par des organismes indépendants. Les activités couvertes par le secret défense sont présentées de manière assez détaillée dans les commissions d'information[46]. Il faut y voir une illustration du mécanisme de la dissuasion nucléaire qui oblige à dire pour intimider l'ennemi ce que l'on veut cacher. Le secret défense, manifestation de souveraineté, est aussi une manière d'écarter : pour les services de la direction de la sécurité intérieure de la préfecture de la région Bourgogne, le secret couvre même les débats de la commission d'information[47]. Le secret nucléaire est une composante de la dissuasion et les opérations de communication, si limitées soient-elles, ne doivent pas faire oublier aux quelques personnes ainsi informées qu'elles sont devant le cœur de la puissance de l'Etat. Le seul intérêt de cette exception au droit commun de la transparence serait de conserver un contrôle discrétionnaire sur le contenu de l'information fournie au public[48]. L'hypothèse doit être formulée car, nonobstant son rôle symbolique, le secret défense présente bien des défauts.

La première de ses faiblesses est son inadaptation aux défis techniques en matière de sécurité des systèmes d'information et de communication. En effet, le secret défense, du moins son encadrement juridique, apparaît anachronique au regard des menaces que les technologies de l'information font peser sur les États souverains et les individus. Le luxe de détail des mesures prévues pour protéger les lieux dédiés aux informations et supports classifiés, la protection des salles de conférences, les mesures spécifiques pour l'accès des magistrats et le rappel des sanctions pénales encourues en cas de divulgation des informations découvertes fortuitement évoquent un cérémonial suranné, indifférent aux évolutions du monde. En novembre 2011, la dernière instruction sur la protection du secret de la défense nationale contient des formulaires de certificats de courriers pour autoriser les convoyeurs à transporter des documents "secret défense". Certes, la protection du secret défense ne se limite pas aux documents classifiés sur support papier, elle s'étend aussi aux moyens informatiques servant à leur élaboration, à leur traitement, à leur stockage et à leur transmission. Cependant, les systèmes d'information présentent des

46 Ainsi, le 6 décembre 2010, devant la commission d'information du CEA Valduc, les grands chantiers prévus sur le site font l'objet d'un power point qui détaille avec bien suffisamment de précision pour le non spécialiste les activités militaires ultra secrètes qui y sont menées ; on y apprend ainsi que l'on poursuit la fabrication de têtes nucléaires aéroportées dans le respect des délais, que le Valduc apporte une contribution importante au programme « tête nucléaire océanique » destinée à équiper les missile M51 en participant à la phase développement et à la conception technologique ainsi qu'aux expériences de simulation, qu'un accord de collaboration entre la France et les USA en neutronique et en criticité permettait d'envisager la mise en place à Valduc d'une nouvelle plate forme expérimentale de criticité unique au monde, enfin que la signature d'un traité de défense franco-britannique relatif au partage d'installations radiographiques et hydrodynamiques communes se traduira par la construction et l'exploitation commune sur le site de Valduc d'une installation radiographique et hydrodynamique, EPURE. Dans le compte rendu du 13 novembre 2012, on apprend aussi que depuis le 12 avril 2012 le centre spécial militaire de Valduc se trouve en période de veille pour une période de deux ans depuis que les objectifs d'assemblage et de désassemblage d'éléments d'armes ont été atteints. La nature des armes en question n'est pas précisée mais le reste du compte rendu permet de comprendre que cela ne signifie pas la fin des fabrications d'armes puisque le centre CEA est chargé de la fabrication des têtes nucléaires océaniques.

47 Dans un compte rendu de la commission d'information du centre CEA Valduc, un participant demande si les membres peuvent faire état des informations qu'ils ont entendues dans les réunions de la commission, oui, lui fut-il répondu, sous réserve de respecter le secret défense. Cf. Commission d'information auprès du Centre d'Energie Atomique de Valduc, réunion du 3 octobre 2007, dans les questions diverses, consultable sur le site de la SEIVA , www.seiva.com.

48 Dans le rapport annuel 2012 du CEAEA, les rejets liquides de Marcoule ne sont pas communiqués car c'est une INBS (installation nucléaire de base secrète). A Valduc, qui est aussi une INBS, les informations sur les rejets liquides sont données : il n'y a pas de rejets liquides.

vulnérabilités propres qui requièrent d'autres précautions. « Ils exigent des règles de sécurité adaptées à l'évolution rapide des techniques et un degré d'expertise de tous les acteurs privés ou publics»[49]. La menace d'une attaque informatique est constante et la compromission d'un secret défense à l'insu même de l'utilisateur est possible à tout moment. En France, le nombre des attaques informatiques traitées par le ministère de la défense est passé de 196 en 2011 à 420 en 2012[50]! Et le vol de données informatiques se pratique couramment[51]. Là où le régime du secret défense prévoit un système de classification et d'habilitation des personnels et des sanctions pénales en cas de compromission du secret, les mesures de sécurité relatives aux systèmes d'information semblent relever d'un tout autre esprit proche de la démarche qualité. Elles privilégient les principes d'organisation et la mise en place de personnes responsables de la sécurité[52]. Défendre l'intégrité de ces systèmes d'information qui innervent aujourd'hui la vie économique et sociale et l'action des pouvoirs publics est un objectif vital. Pourtant, dans le discours des instructions ministérielles, la menace de la sanction pénale s'efface devant les appels pressants à l'analyse des risques, à la sensibilisation, la formation et la responsabilisation des personnels. Si les méthodes de la cyberdéfense sont encore imparfaites[53], il est révélateur de constater qu'elles ne s'inspirent pas des procédés du secret défense.

Le secret défense présente, en outre, de graves défauts. Limité au territoire national, il impose de coûteuses protections physiques et de très indiscrètes procédures d'habilitation. Il s'insinue dans

49 Instruction générale ministérielle n° 1300 sur le secret de la défense nationale du 30 novembre 2011, conclusion de l'introduction, p. 5 et 6.

50 « Des hackers chinois ont pénétré les systèmes informatiques du Pentagone », Le Monde.fr 28 mai 2013. Les pirates informatiques ont eu accès aux plans du système de missiles Patriot, du système de radar ultramoderne Aegis, du chasseur F-18 ou de l'hélicoptère Black Hawk. Plusieurs hauts responsables interrogés par le Washington Post on confirmé que cette attaque était une conséquence d'une vaste campagne d'espionnage chinois contre des industries de la défense et des agences du gouvernement américain. Cyberdéfense : la France reconnaît son retard, Le Monde.fr 3 juin 2013.

51 Pontaut, Jean-Marie, « Un voleur au CEA » « Un sous-traitant informatique soupçonné d'avoir commis un important vol de données confidentielles dans un centre dépendant du Commissariat à l'énergie atomique (CEA) a été placé en garde à vue, le 22 février, au siège de la Direction centrale du renseignement intérieur (DCRI), à Levallois. Le centre où le vol a été commis, situé à Bruyères-le-Châtel (Essonne), est spécialisé dans le calcul de haut niveau. Ses ordinateurs sont notamment utilisés dans le cadre de recherches sur la sûreté des réacteurs nucléaires, l'imagerie médicale ou la climatologie. Selon nos informations, l'affaire a débuté le 31 août 2011, quand les services de sécurité du CEA se sont aperçus que des informations confidentielles venaient d'être recopiées sur des clefs USB. Une plainte a été aussitôt déposée au parquet d'Evry, qui a ouvert une enquête préliminaire. Le suspect, rapidement identifié par la DCRI, a fait l'objet d'une surveillance pendant plusieurs mois afin de connaître ses éventuels contacts. Finalement, il n'aurait pas vendu ces précieuses données, dont le "prix" aurait pu atteindre 20 millions d'euros » L'Express le 14/03/2012 à 18:17

52 Elles prévoient notamment la désignation d'un administrateur de la sécurité habilité secret défense pour chaque système d'information traitant d'informations classifiées et une homologation des systèmes par une commission interne. Dans les articles consacrés aux mesures de sécurité relatives aux systèmes d'information de l'instruction relative au secret défense, il est question d'informer, de sensibiliser, de former et de veiller à la mise en œuvre des mesures de sécurité, il n'est pas fait allusion aux sanctions pénales.

53 Cyberdéfense : la France reconnaît son retard, *Le Monde.fr*, 3 juin 2013, Bockel, Jean Marie, La Cyberdéfense : un enjeu mondial, une priorité nationale, commission des affaires étrangères, de la défense et de forces armées du Sénat, Rapport d'information n°681 (2011-2012) Des progrès ont été fait depuis les rapports Lasbordes et Romani et le Livre blanc sur la défense et la sécurité nationale de 2008 avec la création en juillet 2009 de l'agence nationale de la sécurité des systèmes d'information, agence interministérielle qui est l'autorité nationale de défense des systèmes d'information. Pourtant beaucoup reste à faire dans ce domaine. Manifestement, dans les ministères comme dans les entreprises, la culture de la sécurité des systèmes d'information n'est pas encore bien développée : les personnels chargés de la sécurité des systèmes d'information manquent de considération, d'autorité et de moyens juridiques pour faire respecter les prescriptions. Le ministre de la défense M. Le Drian le reconnaît le 3 juin en Bretagne où une formation d'ingénieurs en cybernétique s'est ouverte en septembre 2013. Cf. Le Monde.fr 3 juin 2013 ; Raphael Baldos, l'école de cyberdéfense ouvrira en septembre, La Croix 3 juin 2013, p. 7.

toutes les entreprises qui doivent être habilitées pour l'exécution de travaux classifiés. Toutes les bases secrètes sont parfaitement visibles sur les cartes satellitaires au même degré de résolution que le reste du territoire tant le « floutage » imposé au titre du secret défense peut aisément être contourné en s'adressant à des sites non français de consultation de cartes. Les sites des installations nucléaires de base secrètes font l'objet de mesures de protection physiques que les textes décrivent avec précision. L'article 413-7 du code pénal punit de six mois d'emprisonnement et de 7500 euros d'amende le fait de s'introduire sans autorisation à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimitées pour assurer la protection des installations, du matériel ou du secret des études ou fabrications. Ces locaux et terrains clos constituent des zones protégées dont l'implantation et les limites sont fixées par arrêté du ministre ayant défini le besoin de protection[54]. La libre circulation y est interdite et l'accès soumis à autorisation. Les limites sont visibles et ne peuvent être franchies par inadvertance. L'ensemble des accès est contrôlé en permanence[55]. L'accès des personnes non qualifiées à ces lieux abritant des secrets de la défense nationale est strictement contrôlé comme celui des personnes effectuant des missions de contrôle. Ainsi les inspecteurs du travail ne sont « nullement autorisés à accéder ou à prendre connaissance des informations classifiées ». Quant aux magistrats, pour effectuer une perquisition dans un lieu précisément identifié comme abritant des éléments classifiés, ils doivent se faire accompagner du président de la commission consultative du secret de la défense nationale qui seul pourra, sans risque de compromission, prendre connaissance des documents classifiés[56]. Ces contrôles d'accès[57] présentent des contraintes sévères pour les personnels non qualifiés secret défense[58] et génèrent des coûts non négligeables[59]. D'autre part, les effets du secret défense sur les marchés publics sont aussi importants. Les procédures d'appel d'offres pour la réalisation de travaux classifiés ou de prestations de services comportant un risque d'accès à des informations classifiées sont rendues anormalement longues et aléatoires pour les entreprises. Les procédures prévues pour les marchés intéressant la défense[60] ne sont pas directement applicables aux marchés du CEA qui relèvent de

54 Article R.413-1à R413-3 du code pénal.

55 C'est ainsi que l'ensemble du centre de Valduc est classé zone protégée, soit pas moins de 700 ha protégés par une série de clôtures, de radars, de caméras, d'interdiction de survol, d'interdiction de photographier et surveillés par un peloton de sécurité et de surveillance de gendarmes mobiles spécialement affectés à la surveillance de Valduc.

56 Article 56-4 du code de procédure pénale.

57 L'accès des personnes non qualifiées pour l'exécution d'une prestation de service, gardiennage, entretien ou maintenance requiert, selon l'article R.413-4 du code pénal, l'autorisation de pénétrer dans la zone protégée donnée par écrit par le chef du service, de l'établissement ou de l'entreprise sous le contrôle du ministre. Il est subordonné à un contrôle élémentaire plus léger que l'habilitation pour garantir que le degré de confiance qu'il est possible de leur accorder est compatible avec les fonctions et les affectations pour lesquelles sont pressenties.

58 Les conséquences sur la vie quotidienne d'un centre sont lourdes. Ainsi les ouvriers qui travaillent sur le chantier d'agrandissement du Centre CEA Valduc ne peuvent pas entrer dans le centre sans être habilités. Donc pour les gros chantiers, comme ceux qui sont actuellement réalisés sur le site de Valduc, il est plus facile d'externaliser le chantier et de créer une entrée indépendante pour en faciliter l'accès. Tous les problèmes ne sont pas réglés pour autant car le restaurant d'entreprise qui pourrait permettre aux ouvriers de se restaurer à midi est dans le centre et donc soumis à un accès contrôlé.

59 Ainsi, une route de deux kilomètres a été créée pour éviter que les ouvriers n'aient à rentrer dans le centre et en subir les contraintes de contrôle liées au secret défense. Par ailleurs, il est interdit d'installer une zone de stationnement pour les véhicules des personnels. Ceux-ci doivent donc être transportés dans des cars affrétés par les entreprises et dans ce cas semble-t-il la durée du transport est décomptée dans les heures de travail.

60 Les marchés publics de défense et de sécurité viennent de faire l'objet d'une réforme suite à la loi n° 2011-702 du 22 juin 2011 relative au contrôle des importations et des exportations de matériels de guerre et de matériels assimilés, à la simplification des transferts de produits liés à la défense dans l'union européenne et aux marchés de défense et de sécurité et au décret n° 2011-1104 du 14 septembre 2011 relatif à la passation et à l'exécution des marchés publics de défense et de sécurité qui insère dans le code des marchés publics une troisième partie relative aux marchés publics de défense et de sécurité.

textes différents mais dont le contenu est assez voisin[61]. Les marchés du CEA passent par une procédure d'appel d'offres qui permet de choisir l'entreprise la mieux disante en fonction des critères choisis. Cependant, les entreprises retenues se trouvent soumises à des exigences particulières. Elles doivent être habilitées confidentiel défense ou secret défense en fonction de l'objet du marché et de son degré d'accès à des informations sensibles sur le site. Cette exigence d'habilitation est contraignante[62] pour les entreprises qui doivent se soumettre à toutes sortes de tracasseries administratives et attendre jusqu'à un an avant de savoir si, en définitive, elles seront retenues pour le marché qu'elles ont obtenu. Elle est contraignante pour le CEA lui-même en termes de délais[63] et de coûts. La procédure d'habilitation est enfin très coûteuse car le CEA entretient des services entiers pour faire ces enquêtes de sécurité[64]. Les auteurs de l'instruction générale n°1300 sur la protection du secret de la défense nationale le reconnaissent en invitant à limiter la prolifération de documents classifiés, à éviter les classifications abusives qui génèrent des coûts de gestion, des charges de travail importantes et altèrent la valeur du secret de la défense nationale[65].

Bien que peu adapté aux nouvelles menaces sur les intérêts vitaux de la nation, le secret défense garde pourtant son prestige auprès des responsables. L'attachement du CEA au secret défense qu'exprime la culture du secret qui pèse sur tous les personnels, sur les sous-traitants et sur les cocontractants même très puissants comme AREVA s'explique sans doute par les avantages qu'il conserve[66]. C'est d'abord un privilège régalien dont bénéficie le CEA, un établissement public industriel et commercial dont les personnels ne sont pas des fonctionnaires. Il témoigne de l'ambition des pionniers de la politique de dissuasion nucléaire comme Pierre Guillaumat de faire de la maîtrise des applications militaires et civiles de l'atome le moyen de restaurer le statut de grande puissance de la France[67]. Créé pour développer les applications de l'énergie nucléaire dans les domaines scientifiques, industriel et de la défense nationale, le CEA est le dépositaire de l'enjeu stratégique de la dissuasion et le gardien du secret défense qui en est une composante essentielle - plus que le gardien d'ailleurs puisque, disposant du secret défense en toute indépendance, il l'impose sans retenue aux autres entreprises[68]. La culture du secret génère

61 Le CEA, établissement public de recherche à caractère scientifique, technique et industriel relevant de la classification des EPIC, n'est pas soumis au code des marchés public mais à l'ordonnance 2005-649 qui transpose la directive européenne 2004/18/CE du 31 mars 2004 et du Décret n° 2005-1742 du 30 décembre 2005 pris en application de cette ordonnance. https://avis-de-marchés.cea.fr/

62 Selon les dires mêmes de M. Régis Baudrillart le directeur du CEA de Valduc qui présentait la procédure d'appel d'offre aux membres de la commission économie de la SEIVA le 16 novembre 2009.
Compte rendu de la commission économie de la SEIVA, lundi 16 novembre 2009, 10 h au CEA de Valduc. Présentation par M Régis Baudrillart du système d'appel d'offres du CEA, centre de Valduc.www.seiva.fr/valduceconomie.htm

63 Le directeur du CEA insiste « c'est une exigence forte et contraignante en termes de délai » car pour obtenir l'habilitation « Confidentiel défense » il faut 4 à 5 mois et pour obtenir l'habilitation « Secret défense », il faut 6 à 7 mois en raison des enquêtes à réaliser sur les personnels, même sur les personnes employées en CDD qui peuvent être habilitées « Secret défense ». A cause du dossier d'habilitation, une affaire peut durer plus d'une année et cette période transitoire coûte cher.

64 Le coût d'une habilitation a été chiffré, c'est assez faramineux. Selon Hervé Cosquer, la Direction centrale de la sécurité du CEA avait évalué, il y a une quinzaine d'années, ce qui renvoie, compte tenu de la date de parution du livre 2007, au début des années 1990, le traitement d'un seul dossier d'habilitation à 3000 francs (environ 450 euros) en coût de personnel et à plus de 10 000 francs (1500 euros) en coût total (personnels, locaux, moyens matériels).

65 Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, chapitre 1er Principe généraux de la classification, Section 1 Les règles de la classification, Responsabilité de la décision de classification, Article 39.

66 Hervé Cosquer, *Les abus du secret défense*, précité.

67 Nicolas Lambert, Avenir radieux, Une fission française, L'échappée 2012 ; L'avenir radieux de l'a-démocratie, Spectacle de la compagnie Un pas de côté, www.unpasdecote.org., Martine Valot, Le Monde, 17 octobre 2012.

68 Hervé Cosquer, *Les abus du secret défense*, précité.

ensuite une culture de la sécurité. La sévérité du régime pénal de la violation du secret défense indique l'importance qui est attachée à sa protection et elle assure l'efficacité des mesures de sensibilisation des personnels à sa protection. Le respect des prescriptions résulte de la peur des poursuites pénales. La pratique quotidienne des contraintes du secret défense confère au personnel cette culture du secret, une vigilance dans les comportements, tant au travail qu'en famille, telle qu'elle produit aussi une culture de la sécurité et une attention aux risques qui ne sont pas seulement ceux de l'espionnage militaire ou industriel[69]. Par la procédure d'habilitation "secret défense", en outre, le secret défense permet de soumettre tout son personnel à des enquêtes à l'embauche d'abord et d'années en années ensuite car l'habilitation n'est que temporaire[70]. Il justifie, aux fins de sécurité de l'habilitation, des atteintes répétées à la vie privée des personnels et de leurs proches. Cette justification par le secret défense des intrusions dans la vie privée des fonctionnaires, des personnels du CEA et des sous-traitants ne bénéficie qu'aux entreprises qui travaillent dans des secteurs protégés par le secret défense. Or l'affaire d'espionnage des salariés et des clients d'Ikea[71] met en évidence l'utilité de ces enquêtes pour les employeurs. Le secret défense, enfin, instaure une sorte de protectionnisme au profit des entreprises inscrites sur la liste des entreprises habilitées secret défense. Il est de nature à permettre le contournement des règles de concurrence pour l'attribution des marchés publics en raison de l'existence d'une liste, elle même classée secret défense, d'entreprises ayant subi avec succès les enquêtes de sécurité nécessaires à l'habilitation secret défense. Ces entreprises déjà habilitées seraient avantagées dans l'attribution des marchés de travaux[72]. Ainsi, en dépit de son inaptitude à répondre aux défis de la sécurité des systèmes d'information, le secret défense conserve des avantages qui expliquent sans doute la considération dont il jouit encore chez les

69 Francois Bugaut, directeur du Centre CEA Valduc, discours prononcé lors de la présentation du bilan des incidents et incendies survenus au CEA Valduc en 2012 à la commission environnement de la SEIVA, www.seiva.fr, le 20 mars 2013, compte rendu sur le site de la SEIVA, p. 6.

70 Les personnels peuvent être soumis à enquête jusqu'à 5 ans après la cessation de leurs fonctions. Ce sont, selon l'instruction 1300, des enquêtes administratives permettant de déceler chez le candidat d'éventuelles vulnérabilités (art. 24, 2 p. 21) Ces enquêtes peuvent concerner aussi les proches des agents car la vulnérabilité peut aussi venir des risques de chantage ou de pressions résultants de menaces sur les proches.(cf. instruction 1300, p. 21) Par le biais de l'annexe de sécurité des contrats passés avec les sous traitants ou les cocontractants, les personnes morales et les dirigeants et les salariés de ces personnes morales sont eux aussi astreints aux procédures d'habilitation "secret défense" et donc aux enquêtes diligentées des services de renseignements (ceux de la direction centrale de sécurité du CEA en l'occurrence pour ne pas charger inconsidérément les services de l'Etat qui sont normalement compétents, la DCRI pour les personnels civils et les organismes travaillant dans le domaine civil, la DPSD et la DGSE pour les personnels militaire et les personnels employés dans des organismes ou entreprises travaillant au profit du ministère de la défense. Cette enquête ayant pour but de détecter la vulnérabilité de la personne à habiliter, l'enquête peut concerner aussi les proches. Le canard enchaîné du 28-03-2012 « En ces temps de menace terroriste, les sous-traitants qui travaillent sur un site sensible pour le compte du Commissariat à l'énergie atomique (CEA), sont priés d'étaler leur vie et celle de leurs proches en guise de laissez-passer. Un courrier récent de la Direction centrale de la sécurité du CEA demande ainsi de fournir une carte d'identité et un CV, mais aussi, "quand cela est possible", l'identité complète avec date et lieu de naissance, nationalité, adresse et profession, de tout ce qui menace à proximité. Et rien sur la race de l'animal de compagnie ? »
http://idata.over-blog.com/4/33/13/76/API/2012-03/29/image0-2012-03-29-18-13-38--0000.jpeg

71 Bertrand Bissuel, La justice met à jour un système d'espionnage à vaste échelle chez Ikea, Le Monde 28/29 juillet 2013.

72 Hervé Cosquer pointe dans son ouvrage sur les abus du secret défense les conséquences du recours abusif selon lui aux procédures d'habilitation des cocontractants. Selon cet ancien commissaire divisionnaire des services centraux des renseignements généraux qui a ensuite dirigé le service de protection du secret et des matières nucléaires à la COGEMA, l'usage excessif du secret défense par le CEA aurait des effets sur l'attribution des marchés. n'est pas plus facile de choisir des sociétés déjà habilitées d'autant que l'habilitation peut durer 5 ans si l'entreprise ne connaît pas de modifications majeures dans son capital. C'est ce que soutient Hervé Cosquer et ce que dément M. Baudrillart qui, interrogé par un membre de la commission économie de la SEIVA qui lui demande : « pour répondre à une offre, la société doit-elle être déjà habilitée ? », répond : « Le CEA ne peut pas sélectionner une société en fonction du critère d'habilitation. Cette méthode serait discriminatoire. »

responsables de la sécurité nucléaire. Ces avantages suffisent-ils à asseoir sa légitimité au regard du droit à l'information du public ?

Le secret défense est toujours opposé au droit à l'information du public en invoquant les exigences de la dissuasion nucléaire et les risques terroristes. La question posée au départ de la recherche sur le secret militaire et la participation était de savoir si la légitimité du secret défense pouvait valablement se mesurer à la légitimité du droit l'information du public sur les activités dangereuses pour la santé ou l'environnement. A l'issue de la recherche et de la réflexion sur les résultats qui a suivi, la légitimité du secret défense apparaît beaucoup moins évidente qu'au premier abord. Largement inefficace en raison de procédures désuètes au regard des menaces qui pèsent sur la sécurité des systèmes informatiques, il peine à justifier sa lourdeur et son coût non seulement pour l'armée et les exploitants d'installations nucléaires intéressant la défense mais encore pour toutes les entreprises et les personnels qui travaillent de près ou de loin pour le nucléaire militaire. Si le secret défense n'assure plus la protection des secrets d'Etat, sa légitimité véritable face au droit de toute personne à être informée des risques des activités pour sa santé et son environnement peut être mise en doute. La faculté de faire des enquêtes sur son personnel, pas plus que le stress salutaire en matière de sécurité et encore moins le contournement des règles de concurrence imposées par le droit européen à la passation des marchés publics ne sauraient fonder le recours au secret défense. Le seul atout véritable du secret défense est la valeur symbolique qui s'attache à ses rites et à ses sanctions. Un symbole prestigieux auxquels les personnels sont attachés quand par ailleurs les activités sont en déclin et que les crédits se font rares. Ce symbole, nous l'avons éprouvé quand, après avoir fait intervenir le ministre de l'écologie, du développement durable et des énergies pour obtenir que notre équipe de chercheurs soit reçue par les responsables du port militaire de Cherbourg, l'officier supérieur chargé de nous présenter les activités du site a indiqué que nous allions voir les installations visitées par les enfants des écoles dans le cadre de la journée du patrimoine ! Et le secret même symbolique n'empêche pas une communication assez précise sur les activités ultra secrètes menées dans les sites couverts par le secret défense. Il est temps d'appliquer à ce secret la règle imposée au militaire non nucléaire et au nucléaire civil qui consiste à fournir au public des informations expurgées de tout élément susceptible de révéler des éléments couverts par le secret défense. Soumettre le secret défense au droit commun de la protection des secrets ne conduirait pas à divulguer au public des informations qui doivent rester confidentielles, cela permettrait seulement de soumettre à l'arbitrage d'un juge les conflits sur la précision des informations à fournir au public. Les conflits entre le droit de savoir et les secrets sont classiques et, dans tous les cas, sauf pour le secret défense, ce sont les juges qui apprécient et tranchent dans le cadre de procédures respectant l'égalité des armes et assurant au requérant des recours, notamment devant le Conseil constitutionnel, la Cour de justice des communautés ou la Cour européenne des droits de l'homme[73].

73 Ces juridictions peuvent faire prévaloir le droit à l'information du public sur le risque avéré d'atteinte à la sécurité publique. Cf. les multiples décisions rendues sur recours de Pierre Azelvandre à propos des pieds de vigne OGM plantés par l'INRA de Colmar sur la commune de Sausheim pour apprécier si le risque d'arrachage des pieds de vigne par les militants anti OGM était une atteinte à l'ordre public susceptible de faire obstacle à la publication en mairie de la localisation exacte des parcelles plantées d'OGM. Billet Philippe, « le régime d'information en matière de localisation des cultures d'OGM, commentaire de CJCE, 17 février 2009, aff. C-552/07 », Cne de Sausheim c/ Pierre Azlvandre, *Dr. rur*. 2009, n°374, comm. p. 121.